Tegucigalpa, MDC,
20 de mayo de 2024

CyC-3410/2024

Señores
OFERENTES
Ciudad

Ref.: CONCURSO PÚBLICO No.05/2024

Estimados señores:

Referente al Concurso Público No.05/2024, para la contratación de los servicios de consultoría para la evaluación del marco de controles de seguridad para el cliente de SWIFT; al respecto, con relación a las consultas realizadas, se remiten las respuestas correspondientes:

- **Consulta No.1:**
  Aclaración Anexo No.2: Condiciones y Requerimientos Técnicos
  1. *¿Qué tipo de arquitectura SWIFT poseen actualmente (A1, A2, A3, A4, B)?*
  2. *¿Cuántas IP internas poseen dentro del segmento SWIFT?*
  3. *¿Cuántos centros de datos poseen?*
  4. *¿Están todos los centros de datos en la misma localidad física? En caso no, por favor especificar ubicaciones.*

  Respuesta
  1. A2.
  2. Entre 65 y 85 IP internas.
  3. Entre 2 y 3 Centros de Datos.
  4. Los Centros de Datos no se encuentran en la misma localidad física y bajo el principio de confidencialidad, la ubicación será proporcionada a la empresa adjudicada una vez sea suscrito el contrato respectivo.

- **Consulta No.2:**
  Requerimientos Técnicos
  Fase II Evaluación del Marco de Controles de Seguridad para el Cliente de SWIFT, Literal a
  Evaluar el cumplimiento de los controles obligatorios y recomendados del Marco de Controles de Seguridad para el Cliente de SWIFT 2024 o 2025 (según los tiempos de presentación o las necesidades que el Banco establezca), bajo una metodología basada en Riesgos tal y como se define en el Marco de Evaluación Independiente (IAF, por sus siglas en inglés) y bajo una estrategia de Defensa en Profundidad.

  1. *¿Se desea evaluar contra SWIFT 2024 o 2025?*

2. *¿Se desea únicamente un análisis de brechas contra los lineamientos de SWIFT y/o la auditoria de cumplimiento?*
3. *¿Se encuentran actualmente en cumplimiento?*

Respuesta

1. Se desea evaluar contra SWIFT 2024. Sin embargo, si debido a factores externos al BCH los servicios de consultoría comenzaran a ejecutarse en el año 2025, se deberá evaluar contra SWIFT 2025.
2. La empresa SWIFT en su Marco de Evaluación Independiente, numeral 4.1 "Enfoque de auditoría frente a evaluación", menciona que: "Swift ha optado por un enfoque de revisión de "evaluación" en lugar de "auditoría" para el CSP...". Por lo anterior, se debe evaluar el cumplimiento de la eficacia del diseño y la aplicación de los controles mediante la metodología de evaluación descrita en el Marco de Evaluación Independiente.
3. El BCH se encuentra actualmente en cumplimiento.

- **Consulta No.3:**
  Requerimientos Técnicos
  Fase III Concientización en Seguridad de la Información y Ciberseguridad, Literal b
  Considerando los resultados obtenidos en el inciso a) se deben impartir charlas de concientización y capacitación, según el esquema siguiente:

  - *Una (1) charla de concientización sobre Seguridad de la Información y Ciberseguridad dirigida al Comité de Riesgos y Directorio del BCH, misma que debe tener una duración de una (1) hora aproximadamente.*
  - *Una (1) charla de concientización sobre Seguridad de la Información y Ciberseguridad dirigida al nivel operativo, misma que debe tener una duración de dos (2) horas aproximadamente.*
  - *Un (1) taller de capacitación en Ciberseguridad dirigida al nivel técnico del BCH, misma que debe tener una duración de ocho (8) horas aproximadamente.*

  1. *¿Cuántas personas formarían parte de las charlas de concientización tanto en la dirigida a comité y directorio, como la dirigida a nivel operativo, respectivamente?*
  2. *¿Cuáles son las expectativas del taller de capacitación dirigida a nivel técnico?*
  3. *¿Qué tema se desea evaluar tras el taller?*
  4. *¿Está la evaluación incluida dentro de las 8 horas de taller o deben considerarse adicionales?*
  5. *¿Cuántas personas serán parte de este taller dirigido al nivel técnico?*

  Respuesta

  1. Entre 18 y 23 personas formarían parte de la charla de concientización dirigida al Comité de Riesgos y Directorio del BCH y entre 23 y 28 personas formarían parte de la charla de concientización dirigida a nivel operativo.
  2. Capacitar al personal técnico en temas de ciberseguridad, entre ellos:
     - Panorama mundial de riesgos cibernéticos y tendencias en tecnologías de protección

Centro Cívico Gubernamental, Frente Bulevar de las Fuerzas Armadas,
Apartado Postal No. 3165, Tegucigalpa, MDC, Honduras
P.B.X. (504) 2262-3700
www.bch.hn

- Mejores prácticas de Ciberseguridad para la protección de la infraestructura tecnológica del BCH (incluida la infraestructura de SWIFT), entre ellas: el endurecimiento de equipos de TI, gestión de vulnerabilidades, monitoreo de eventos.
- Roles y responsabilidades de seguridad.
- Gestión eficiente de incidentes cibernéticos.
- Últimas tendencias en tecnologías de protección

3. Los temas mencionados de la respuesta anterior
4. La evaluación está incluida en las 8 horas de taller.
5. Entre 20 y 25 personas formarían parte del taller dirigido al nivel técnico

- **Consulta No.4:**
  Requerimientos Técnicos
  Fase II Evaluación del Marco de Controles de Seguridad para el Cliente de SWIFT, Literal b
  Realizar un análisis de vulnerabilidades, pruebas de intrusión y revisión de endurecimiento de TI dentro del alcance del entorno SWIFT, mediante el uso de herramientas manuales y automatizadas; en el caso de las pruebas de intrusión, el oferente debe utilizar técnicas de hacking ético.

  En apartado referente a Revisión de Endurecimiento de TI, ¿Cómo se desea qué se ejecute esta revisión, con revisión de guías de hardening, análisis de vulnerabilidades, revisión de configuraciones? por favor ampliar la expectativa de esa revisión.

  Respuesta
  La revisión debe realizarse a través de herramientas tecnologías especializadas y diseñadas para la revisión de Endurecimiento (Hardening), que permitan identificar debilidades en la configuración de seguridad de los equipos de TI, que se encuentre dentro del alcance del entorno SWIFT.

- **Consulta No.5:**
  Anexo I Condiciones Específicas del Concurso
  Numeral 7 Plan de Trabajo
  *El oferente debe considerar entre el cierre de la Fase II: Evaluación del Marco de Controles de Seguridad para el Cliente de SWIFT y la Fase IV: Cierre, debe existir una diferencia de tiempo no menor a **tres (3) meses**, para que permita al Banco realizar las actividades indicadas en el "Plan de Remediación" para las posibles vulnerabilidades identificadas en la implementación del Marco de Controles de Seguridad para el Cliente de SWIFT.*

  ¿Se considera el tiempo de remediación por parte del banco (3 meses) dentro de los 5 meses plazo de ejecución del proyecto?

  Respuesta
  El tiempo de remediación por parte del BCH (al menos 3 meses) debe estar contemplado dentro de los 5 meses plazo de ejecución de la consultoría.

- **Consulta No.6:**
  General: Confirmar si se cuenta con un presupuesto base que se deba tener en cuenta como parte de los análisis realizados para la presentación de la oferta comercial del servicio.

  Respuesta
  El Banco Central de Honduras cuenta con un presupuesto base para la ejecución de los servicios de consultoría; sin embargo, el mismo es de carácter confidencial.

- **Consulta No.7:**
  General: Confirmar la fecha estimada de inicio del servicio, una vez adjuntado el contrato.

  Respuesta
  Si el Concurso Público se desarrolla de forma normal, se estimada que la adjudicación sea en el mes de julio del 2024, posteriormente, se debe suscribir y aprobar el contrato de acuerdo con el tiempo mencionado en el numeral 10.2.1 de los TDR que norman este concurso; posterior a ello, el Gerente de Proyecto del BCH emite la orden de inicio para el servicio de consultoría.

- **Consulta No.8:**
  Términos de Referencia - Sección 5: Solicitamos amablemente que se posponga la fecha de entrega de la propuesta/oferta hasta el 31 de mayo de 2024. Esta extensión nos permitirá elaborar una propuesta alineada con sus necesidades y llevar a cabo los procesos internos administrativos y de calidad, teniendo en cuenta el sector al que pertenece el Banco Central.

  Respuesta
  La recepción de ofertas se realizará en la fecha que sea establecido en los Términos de Referencia del Concurso Público No.05/2024.

- **Consulta No.9:**
  Términos de Referencia - Sección 5: Solicitamos evaluar la posibilidad de aceptar la presentación de las propuestas de servicio y la documentación asociada (documentación técnica, documentación legal y oferta económica) por medio de canales digitales como correo electrónico.

  Respuesta
  Las ofertas deben ser presentadas conforme a lo establecido en los Términos de Referencia, Numeral 1. DE LAS OFERTAS y Numeral 3. PRESENTACIÓN DE LAS OFERTAS.

- **Consulta No.10:**
  Anexo 01 - Numeral 1: Confirmar el tipo de arquitectura operativa de la entidad (A o B)

  Respuesta
  Ver respuesta en consulta No.1, numeral 1.

- **Consulta No.11:**
  Anexo 01 - Numeral 2: Confirmar la cantidad de activos de información que conforman el entorno SWIFT, que deben ser incluidos como parte del análisis de riesgos asociados a la Seguridad de la Información y Ciberseguridad. Esta información es necesaria para estimar los tiempos y esfuerzo adecuado para ejecutar esta actividad.

  Respuesta
  Entre 65 y 85 activos de información

- **Consulta No.12:**
  Anexo 01 - Numeral 2: Describir de forma general la metodología de Análisis de Riesgos definida por el BCH, que debe ser ejecutada como parte del análisis de riesgos asociados a la Seguridad de la Información y Ciberseguridad. Esta información es necesaria para estimar los tiempos y esfuerzo adecuado para ejecutar esta actividad.

  Respuesta
  La metodología de Análisis de Riesgos comprende al menos las siguientes fases: Identificación y valoración de activos de información; Identificación de riesgos, Análisis de riesgos, Evaluación del riesgo, Tratamiento del riesgo y Seguimiento.

- **Consulta No.13:**
  Anexo 01 - Numeral 2: Confirmar si el BCH ha realizado un análisis para garantizar que no existan conflictos de interés ni conflictos funcionales en la ejecución de los objetivos específicos del servicio. Esta consulta se realiza dado que, como parte de la Evaluación del Marco de Controles de Seguridad para el Cliente de SWIFT, se deben revisar y evaluar los siguientes controles y al mismo tiempo, el servicio requerido incluye actividades de definición e implementación de dichos controles: - Control 7.4.A: Evaluación de escenarios de riesgos - Control 7.2: Capacitación y concientización en materia de seguridad - Control 2.7: Escaneo de vulnerabilidades.

  Respuesta
  El BCH evita los conflictos de interés y funcionales a través de la supervisión de las actividades desarrollas y realizará revisión de los entregables que forman parte de los servicios de consultoría.

- **Consulta No.14:**
  Anexo 1 - Numeral 4.4: Con respecto al numeral 4.4, por favor confirmar si los entregables de cada fase deben ser entregados de forma física en las instalaciones del BCH o si pueden ser entregados de forma digital/electrónica a través de medios que cuenten con medidas de protección adecuadas.

  Respuesta
  Se confirma que los entregables deben ser entregados en el edificio del BCH ubicado en el Bulevar Fuerzas Armadas en la capital, efectuando lo establecido en los numerales 4.3, 4.4 y 4.5 del Anexo 1.

Centro Cívico Gubernamental, Frente Bulevar de las Fuerzas Armadas,
Apartado Postal No. 3165, Tegucigalpa, MDC, Honduras
P B X. (504) 2262-3700
www.bch.hn

- **Consulta No.15:**
  Anexo 1 - Numeral 6.5.1
  Certificaciones mínimas requeridas para el rol de Especialista en evaluación de controles de seguridad: Evaluar la posibilidad de incluir como parte de las certificaciones mínimas aceptadas para este cargo, el combo de certificaciones ISO27001 Lead Auditor + ISO27001 Lead Implementer. Esto teniendo en cuenta que el servicio requerido requiere conocimientos específicos no solo en implementación de SGSI sino en la evaluación adecuada de los mismos, así como habilidades para proponer acciones de mejora basados en este framework de seguridad. Un profesional que cuente con estas dos certificaciones, cuenta además con habilidades para evaluar la adecuación y eficacia del SGSI en términos de la gestión de riesgos, controles de seguridad, políticas y procedimientos, más allá de solo una evaluación tecnológica. Así mismo, está capacitado para realizar auditorías internas y externas del SGSI, identificar áreas de mejora y promover la mejora continua del sistema.

  Respuesta
  Conforme a los Términos de Referencia del Concurso Público No.05/2024, la certificación ISO/IEC 27001 Lead Auditor es la solicitada, mientras que para la certificación ISO/IEC 27001 Lead Implemeter se requiere que la credencial sea Senior.

- **Consulta No.16:**
  Anexo 1 - Numeral 6.5.1
  Certificaciones mínimas requeridas para el rol de Especialista en análisis de vulnerabilidades, pruebas de intrusión y revisión de endurecimiento de TI: Evaluar la posibilidad de incluir como parte de las certificaciones mínimas aceptadas para este cargo, la certificación de CompTIA Security que brinda un enfoque más integral y técnico en pruebas de penetración y ciberseguridad. Los profesionales con esta certificación cuentan con habilidades y conocimientos fundamentales en seguridad de la información y ciberseguridad. Está capacitado para comprender los conceptos básicos de seguridad cibernética, evaluar y gestionar riesgos, implementar tecnologías de seguridad, mantener una infraestructura de red segura, entender principios de criptografía, manejar incidentes de seguridad, identificar vulnerabilidades en aplicaciones, y comunicarse efectivamente sobre temas de seguridad.

  Respuesta
  Conforme a los Términos de Referencia del Concurso Público No.05/2024, la certificación CompTIA Security+ es la solicitada.

- **Consulta No.17:**
  Anexo 2 - Numeral 1
  Requerimiento - Evaluación del Marco de Controles de Seguridad para el Cliente de SWIFT. Con respecto a la actividad "Realizar un análisis de vulnerabilidades, pruebas de intrusión y revisión de endurecimiento de TI dentro del alcance del entorno SWIFT", por favor confirmar: - Cantidad aproximada de direcciones IPS para el análisis de vulnerabilidades - Cantidad aproximada de direcciones IPS para el pruebas de intrusión - Cantidad de sistemas operativos por revisar en las

pruebas de endurecimiento de TI (Hardening) - Confirmar si el alcance del análisis de vulnerabilidades y pruebas de intrusión contempla solo la red interna.

Respuesta
La cantidad aproximada de direcciones IPS para el análisis de vulnerabilidades, pruebas de intrusión, pruebas de endurecimiento de TI (Hardening) es entre 65 y 85. Asimismo, se confirma que el alcance del análisis de vulnerabilidades y pruebas de intrusión contempla solo la red interna.

- **Consulta No.18:**
  Anexo 2 - Numeral 1
  Requerimiento - Concientización en Seguridad de la Información y Ciberseguridad. Con respecto a la actividad "Evaluar el grado actual de conciencia en Seguridad de la Información y Ciberseguridad del personal técnico y operativo, a través de la aplicación de pruebas de conocimiento e ingeniería social", por favor confirmar si se espera como parte del servicio la ejecución de pruebas de ingeniería social (pruebas de Phishing o similares). Si es así, por favor confirmar el alcance de estas pruebas.

  Respuesta
  Se requiere la ejecución de pruebas de ingeniería social, que incluyan al menos pruebas de phishing y vishing.

- **Consulta No.19:**
  Anexo 2 - Numeral 1
  Requerimiento - Concientización en Seguridad de la Información y Ciberseguridad. Con respecto al taller de capacitación en Ciberseguridad dirigida al nivel técnico del BCH, confirmar los temas técnicos que se requieren incluir como parte de la capacitación y las características de la misma.

  Respuesta
  Ver respuesta en consultas No. 3 y 26; asimismo, los temas deben ser abordados de forma teórica incluyendo ejemplos reales que permitan mejorar su comprensión; asimismo, de ser posible se deben incluir ejercicios prácticos.

- **Consulta No.20:**
  Entender si la evaluación del marco SWIFT es completa, ¿es decir los 32 controles?

  Respuesta
  La evaluación del marco SWIFT debe incluir los 32 controles, según lo establecido en el Anexo No.2, Numeral 1, Sección I, Fase II, inciso a).

- **Consulta No.21:**
  Cantidad de IP's/Assets para pruebas de vulnerabilidades de ambiente SWIFT

Respuesta
Entre 65 y 85 IP's/Assets.
Ver respuesta consulta No.1, numeral 2

- **Consulta No.22:**
Tipo de pruebas de intrusión (interna o externa o ambas) y cantidad de IP's/Assets/Redes I

Respuesta
El tipo de prueba de intrusión es interna e incluye entre 65 y 85 IP's.

- **Consulta No.23:**
Cantidad de dispositivos que puedan ser incluidos en el proceso de hardening del ambiente SWIFT

Respuesta
Ver respuesta de consulta No.1, numeral 2

- **Consulta No.24:**
Cantidad de usuarios para la capacitación

Respuesta
Ver respuesta en consulta No. 3

- **Consulta No.25:**
Tipo de capacitación (Remota o presencial)

Respuesta
Presencial, considerando el tiempo mínimo de estadía por fase establecido en los Términos de Referencia, numeral 12, subnumeral 12.1.1.

- **Consulta No.26:**
Hay necesidad de certificación para usuario final en capacitación o para el usuario técnico

Respuesta
Se debe emitir Certificados de Participación según lo establecido en el Anexo No.2, Numeral 1, Sección II, Fase III, inciso b).

- **Consulta No.27:**
¿Capacitación técnica requerida para personal técnico?

Respuesta
Los temas deben ser abordados de forma teórica incluyendo ejemplos reales que permitan mejorar su comprensión; asimismo, de ser posible se deben incluir ejercicios prácticos.
Ver respuesta de consulta No.3

- **Consulta No.28:**
  Pruebas de phishing – Cuantos mails box se tienen que incluir

  Respuesta
  Entre 43 y 53.

- **Consulta No.29:**
  Pruebas de phishing continuas o un one time

  Respuesta
  Pruebas de phishing one time.

Atentamente,

FANNY MARISABEL TURCIOS BARRIOS
Secretaria Comisión de Compras y Evaluación y
Jefe Departamento de Compras y Contrataciones

IMP/KAC/OMC